




ELECTRONIC INFORMATION DISCLOSURE STATEMENT

Electronic Version v18

Stylesheet Version v18.0

| Title of Invention | Attestation Key Memory Device and Bus | | | | | | |
|--|---------------------------------------|-------------|------------|----------------------------------|------|-------|----------|
| <div>Application Number: 09/541667</div> <div>Confirmation Number: 3630</div> <div>First Named Applicant: Carl Ellison</div> <div>Attorney Docket Number: 42P08629</div> <div>Art Unit: Unknown</div> <div>Examiner: Unknown Unknown</div> <div>Search string: (20030018892 or 4162536 or 4247905 or 4276594 or 4307447 or 4347565 or 4759064 or 4795893 or 4825052 or 4907270 or 4907272 or 4910774 or 5007082 or 5139760 or 5317705 or 5319760 or 5434999 or 5437033 or 5442645 or 5504922 or 5511217 or 5522075 or 5528231 or 5533126 or 5566323 or 5606617 or 5720609 or 5721222 or 5737604 or 5796835 or 5825875 or 5854913 or 5867577 or 5900606 or 5901225 or 5903752 or 6061794 or 6075938 or 6092095 or 6182089 or 6212635 or 6222923 or 6269392 or 6272637 or 6308270 or 6314409 or 6330670 or 6363485 or 6374286 or 6374317 or 6378072 or 6397242 or 6412035 or 6421702 or 6435416 or 6445797 or 6463537 or 6557104).pn.</div> <div></div> <div>RECEIVED JAN 28 2004 Technology Center 2100</div> | | | | | | | |
| US Patent Documents | | | | | | | |
| Note: Applicant is not required to submit a paper copy of cited US Patent Documents | | | | | | | |
| init | Cite.No. | Patent No. | Date | Patentee | Kind | Class | Subclass |
| h | 1 | 20030018892 | 2003-01-23 | Tello, Jose | | | |
| h | 2 | 4162536 | 1979-07-24 | Morley, Richard E. | | | |
| m | 3 | 4247905 | 1981-01-27 | Yoshida, Yukihiro , et al. | | 711 | 166 |
| m | 4 | 4276594 | 1981-06-30 | Morley, Richard E. | | | |
| m | 5 | 4307447 | 1981-12-22 | Provanzano, Salvatore R., et al. | | | |
| h | 6 | 4347565 | 1982-08-31 | Kaneda, Saburo , et al. | | | |
| m | 7 | 4759064 | 1988-07-19 | Chaum, | | | |
| | | | | | | | |

| | | | | |
|---|----|---------|------------|-------------------------------|
| h | 8 | 4795893 | 1989-01-03 | Ugon, Michael |
| m | 9 | 4825052 | 1989-04-25 | Chemin, Francois , et al. |
| m | 10 | 4907270 | 1990-03-06 | Hazard, Michel |
| m | 11 | 4907272 | 1990-03-06 | Hazard, Michel |
| m | 12 | 4910774 | 1990-03-20 | Barakat, Simon |
| h | 13 | 5007082 | 1991-04-09 | Cummins, Mary T. |
| h | 14 | 5139760 | 1994-06-07 | Mason, Andrew H., et al. |
| m | 15 | 5317705 | 1994-05-31 | Gannon, Patrick M., et al. |
| m | 16 | 5319760 | 1994-06-07 | Mason, Andrew H., et al. |
| m | 17 | 5434999 | 1995-07-18 | Goire, Christian , et al. |
| h | 18 | 5437033 | 1995-07-25 | Inoue, Taro , et al. |
| m | 19 | 5442645 | 1995-08-15 | Ugon, Michel , et al. |
| m | 20 | 5504922 | 1996-04-02 | Seki, Yukihiro , et al. |
| h | 21 | 5511217 | 1996-04-23 | Nakajima, Atsushi , et al. |
| m | 22 | 5522075 | 1996-05-28 | Robinson, Paul T., et al. |
| m | 23 | 5528231 | 1996-06-18 | Patarin, Jacques |
| m | 24 | 5533126 | 1996-07-02 | Hazard, Michel , et al. |
| m | 25 | 5566323 | 1996-10-15 | Ugon, Michel |
| m | 26 | 5606617 | 1997-02-25 | Brands, Stefanus A. |
| h | 27 | 5720609 | 1998-02-24 | Pfefferle, William C. |
| h | 28 | 5721222 | 1998-02-24 | Bernstein, Peter R., et al. |
| m | 29 | 5737604 | 1998-04-07 | Miller, David A., et al. |
| m | 30 | 5796835 | 1998-08-18 | Saada, Charles |
| m | 31 | 5825875 | 1998-10-20 | Ugon, Michel |
| h | 32 | 5854913 | 1998-12-29 | Goetz, John W., et al. |
| m | 33 | 5867577 | 1999-02-02 | Patarin, Jacques |
| m | 34 | 5900606 | 1999-05-04 | Rigal, Vincent |
| m | 35 | 5901225 | 1999-05-04 | Ireton, Mark A., et al. |
| m | 36 | 5903752 | 1999-05-11 | Dingwall, Thomas J., et al. |
| m | 37 | 6061794 | 2000-05-09 | Angelo, Michael E. |
| h | 38 | 6075938 | 2000-06-13 | Bugnion, Edouard , et al. |
| m | 39 | 6092095 | 2000-07-18 | Maytal, Benjamin |
| m | 40 | 6182089 | 2001-01-30 | Ganapathy, Narayanan , et al. |
| m | 41 | 6212635 | 2001-04-03 | Reardon, David C. |
| m | 42 | 6222923 | 2001-04-24 | Schwenk, Joerg |
| h | 43 | 6269392 | 2001-07-31 | Cotichini, Christian , et al. |
| | | | | |

| | | | | | |
|----|---------|------------|----------------------------|-----|-----|
| 44 | 6272637 | 2001-08-07 | Little, Wendell L., et al. | 713 | 194 |
| 45 | 6308270 | 2001-10-23 | Guthery, Scott B., et al. | | |
| 46 | 6314409 | 2001-11-06 | Schneck, Paul B., et al. | | |
| 47 | 6330670 | 2001-12-11 | England, Paul , et al. | | |
| 48 | 6363485 | 2002-03-26 | Adams, Carlisle | | |
| 49 | 6374286 | 2002-04-16 | Gee, John K., et al. | | |
| 50 | 6374317 | 2002-04-16 | Ajanovic, Jasmin , et al. | 710 | 105 |
| 51 | 6378072 | 2002-04-23 | Collins, Thomas , et al. | | |
| 52 | 6397242 | 2002-05-28 | Devine, Scott W., et al. | | |
| 53 | 6412035 | 2002-06-25 | Webber, Victor | | |
| 54 | 6421702 | 2002-07-16 | Gulick, Dale E. | | |
| 55 | 6435416 | 2002-08-20 | Slassi, Tarik | | |
| 56 | 6445797 | 2002-09-03 | McGough, Paul , et al. | | |
| 57 | 6463537 | 2002-10-08 | Tello, Jose A. | | |
| 58 | 6557104 | 2003-04-29 | Vu, Son T., et al. | | |

Remarks

Note: Remarks are not for responding to an office action.

Applicants, in accordance with their duty of disclosure under 37 CFR 1.56 and in accordance with 37 CFR 1.97(c)(2), hereby submit this Electronic Information Disclosure Statement citing U.S. Patent documents for consideration by the Examiner. Pursuant to 37 CFR 1.97, the submission of this Electronic Information Disclosure Statement is not to be construed as a representation that a search has been made and is not to be construed as an admission that the information cited in this statement is material to patentability. This Electronic Information Disclosure Statement is being filed after the mailing of a first office action and before the mailing of a final office action, notice of allowance, or an action otherwise closing prosecution. Pursuant to 37 CFR 1.97(c)(2), the fee set forth in 37 CFR 1.17(p) of \$180.00 is due for the filing of this Electronic Information Disclosure Statement. Please charge this fee and any other fee that may be due to Deposit Account 02-2666. Applicants respectfully request that the cited documents be considered and that the form be initialed by the Examiner to indicate such consideration and a copy thereof be returned to Applicants' attorney of record.

Signature

| | |
|---------------|------|
| Examiner Name | Date |
|---------------|------|

#14

PTO/SB/08A(10-01)

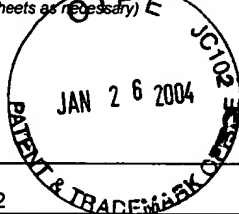
Approved for use through 10/31/2002. OMB 651-0031
US Patent & Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**

(Use as many sheets as necessary)



Complete if Known

| | |
|----------------------|----------------|
| Application Number | 09/541667 |
| Filing Date | March 31, 2000 |
| First Named Inventor | Ellison, Carl |
| Group Art Unit | Unknown |
| Examiner Name | Unknown |

RECEIVED

JAN 28 2004

Sheet 1 of 2

Attorney Docket No: 42P08629

Technology Center 2100

US PATENT DOCUMENTS

| Examiner Initial * | USP Document Number | Publication Date | Name of Patentee or Applicant of cited Document | Class | Subclass | Filing Date if Appropriate |
|--------------------|---------------------|------------------|---|-------|----------|----------------------------|
|--------------------|---------------------|------------------|---|-------|----------|----------------------------|

FOREIGN PATENT DOCUMENTS

| Examiner Initials* | Foreign Document No | Publication Date | Name of Patentee or Applicant of cited Document | Class | Subclass | T ² |
|--------------------|---------------------|------------------|---|-------|----------|----------------|
| n | DE-4217444 | 12/03/1992 | Toyohisa, Imada, et al. | | | |
| n | EP-0473913 | 03/11/1992 | Farrell, Joel A. | | | |
| n | JP-2000076139 | 03/14/2000 | Tanno, Masaaki, et al. | | | |
| n | WO-0175564 | 10/11/2002 | Herbert, Howard C., et al. | | | |
| n | WO-02086684 | 10/31/2002 | Proudlar, Graeme J. | | | |
| n | WO-0217555 | 02/28/2002 | Ford, Warwick | | | |

OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS

| Examiner Initials* | Cite No ¹ | Include name of the author (In CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published. | T ² |
|--------------------|----------------------|--|----------------|
| n | | BRANDS, STEFAN, "Restrictive Blinding of Secret-Key Certificates", SPRINGER-VERLAG XP002201306, (1995), Chapter 3 | |
| n | | CHIEN, ANDREW A., et al., "Safe and Protected Execution for the Morph/AMRM Reconfigurable Processor", 7th Annual IEEE Symposium, FCCM '99 Proceedings, XP010359180, ISBN 0-7695-0375-6, Los Alamitos, CA, (4/21/1999), 209-221 | |
| n | | COMPAQ COMPUTER CORPORATION, et al., "Trusted Computing Platform Alliance (TCPA) Main Specification Version 1.1a", (12/2001), 1-321 | |
| n | | DAVIDA, GEORGE I., et al., "Defending Systems Against Viruses through Cryptographic Authentication", Proceedings of the Symposium on Security and Privacy, IEEE Comp. Soc. Press, ISBN 0-8186-1939-2, (May 1989), | |
| n | | IBM, "Information Display Technique for a Terminate Stay Resident Program IBM Technical Disclosure Bulletin", TDB-ACC-No. NA9112156, Vol. 34, Issue 7A, (12/1/1991), 156-158 | |
| n | | KARGER, PAUL A., et al., "A VMM Security Kernel for the VAX Architecture", Proceedings of the Symposium on Research in Security and Privacy, XP010020182, ISBN 0-8186-2060-9, Boxborough, MA, (5/7/1990), 2-19 | |
| n | 0 | KASHIWAGI, KAZUHIKO, et al., "Design and Implementation of Dynamically Reconstructing System Software", Software Engineering Conference, Proceedings 1996 Asia-Pacific Seoul, South Korea 4-7 Dec. 1996, Los Alamitos, CA USA, IEEE Comput. Soc. US, ISBN 0-8186-7638-8, (1996), | |
| n | | LUKE, JAHN, et al., "Replacement Strategy for Aging Avionics Computers", IEEE AES Systems Magazine, XP002190614, (March 1999), | |
| n | | MENEZES, OORSCHOT, "Handbook of Applied Cryptography", CRC Press LLC, USA XP002201307, (1997), 475 | |
| n | | RICHT, STEFAN, et al., "In-Circuit-Emulator Wird Echtzeitauglich", Elektronik, | |

EXAMINER

n

DATE CONSIDERED

2/25/04

Substitute Disclosure Statement Form (PTO-1449)

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional) 2 Applicant is to place a check mark here if English language Translation is attached

#14

PTO/SB/08A(10-01)

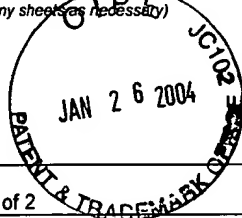
Approved for use through 10/31/2002. OMB 851-0031
US Patent & Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**

(Use as many sheets as necessary)



Complete if Known

Application Number 09/541667

Filing Date March 31, 2000

First Named Inventor Ellison, Carl

Group Art Unit Unknown

Examiner Name Unknown

RECEIVED

JAN 28 2004

Technology Center 2100

Sheet 2 of 2

Attorney Docket No: 42P08629

OTHER DOCUMENTS -- NON PATENT LITERATURE DOCUMENTS

| Examiner Initials* | Cite No ¹ | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published. | T ² |
|--------------------|----------------------|---|----------------|
| n | | Franzis Verlag GMBH, Munchen, DE, Vol. 40, No. 16, XP000259620, (100-103), 8-6-1991 | |
| n | | ROBIN, JOHN S., et al., "Analysis of the Pentium's Ability to Support a Secure Virtual Machine Monitor", <u>Proceedings of the 9th USENIX Security Symposium</u> , XP002247347, Denver, Colorado, (8/14/00), 1-17 | |
| n | | SAEZ, SERGIO, et al., "A Hardware Scheduler for Complex Real-Time Systems", <u>Proceedings of the IEEE International Symposium on Industrial Electronics</u> , XP002190615, (July 1999), 43-48 | |
| n | | SHERWOOD, TIMOTHY, et al., "Patchable Instruction ROM Architecture", <u>Department of Computer Science and Engineering, University of California, San Diego, La Jolla, CA, (Nov. 2001)</u> , | |

EXAMINER

DATE CONSIDERED

2/28/04

Substitute Disclosure Statement Form (PTO-1449)

* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (optional) 2 Applicant is to place a check mark here if English language Translation is attached